UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

SHANNAN ELLIS, individually and on behalf of all others similarly situated, Plaintiff, vs. HUB INTERNATIONAL LIMITED, Defendant.	CASE NO. **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Shannan Ellis ("Plaintiff") brings this action on behalf of herself, and all others similarly situated against Defendant, HUB International Limited ("HUB" or "Defendant"), and alleges as follows:

I. INTRODUCTION

1. This lawsuit stems from a massive and preventable data breach spanning from December 2022 through January 2023 in which cybercriminals infiltrated HUB's inadequately protected network systems and accessed the highly sensitive personally identifiable information ("PII") of approximately **479,261 individuals** (the "Data Breach" or Breach").[1]

2. According to HUB the Data Breach began in or around December 2022,

[1] *See* https://apps.web.maine.gov/online/aeviewer/ME/40/a5e4c9cb-5a57-4d11-aa3a-88c06e7a220d.shtml.

but was not discovered by HUB until January 17, 2023.[2]

3. After an investigation, HUB determined that the types of PII accessed and copied by cybercriminals during the Data Breach included, *inter alia*, names, Social Security numbers, driver's license numbers, passport numbers, and financial account information.[3]

4. On August 11, 2023 – 7 months after the unauthorized party first gained access to Plaintiff and the Class's PII – victims of the Data Breach were finally notified via letter that their highly sensitive and confidential PII was exposed ("Notice of Data Breach Letter"). [4]

5. The Notice of Data Breach Letter obscured the nature of the breach and the threat it posed—failing to notify Plaintiff and the Class how many people were impacted, how the Breach happened, or why it took so long to begin notifying victims that hackers had gained access to highly sensitive PII.

6. Defendant's failure to timely detect and report the Data Breach made the victims vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their PII.

7. Defendant knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the

[2] *See* Exhibit 1.

[3] *Id.*; *see also* https://dataconomy.com/2023/08/15/hub-international-data-breach/.

[4] *See* Exhibit 1.

effects of PII misuse.

8. In failing to adequately protect Plaintiff's and the Class's PII, failing to adequately notify them of the Breach, and by obfuscating the nature of the breach, Defendant violated state and federal laws and harmed Plaintiff and the Class.

9. Plaintiff and members of the proposed Class are victims of Defendant's negligence and inadequate cyber security measures.

10. Moreover, HUB failed to properly use up-to-date security practices to prevent the Data Breach.

11. Plaintiff Shannan Ellis is a Data Breach victim.[5]

12. Accordingly, Plaintiff, on her own behalf and on behalf of a class of similarly situated individuals, brings this lawsuit seeking injunctive relief, damages, and restitution, together with costs and reasonable attorneys' fees, the calculation of which will be based on information in Defendant's possession.

II. PARTIES

13. Plaintiff, **Shannan Ellis**, is a natural person and citizen of Minnesota, where she intends to remain. Plaintiff is a Data Breach victim and received a Notice of Data Breach Letter informing her that her Social Security number was compromised.[6]

14. Defendant, **HUB**, is a corporation registered with the Illinois Secretary of State, with its principal place of business believed to be located at 150 N. Riverside Plaza,

[5] *See id.*

[6] *Id.*

17th Floor, Chicago, IL 60606.

III. JURISDICTION & VENUE

15. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and Plaintiff and Defendant are citizens of different states.

16. This Court has personal jurisdiction over Defendant because Defendant maintains its principal place of business in this District and does substantial business in this District.

17. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claim occurred in this District.

IV. FACTUAL ALLEGATIONS

The Data Breach

18. HUB is an insurance brokerage company based in Chicago, Illinois.[7] HUB provides various types of insurance through its marketplace, including property casualty, risk management, life and health, reinsurance, and employee benefits services.[8] HUB employs more than 16,000 people and generates approximately $7.5 million in annual

[7] https://www.jdsupra.com/legalnews/hub-international-limited-files-notice-7826466/.

[8] *Id.*

revenue.[9]

19. Through the services HUB provided, Defendant collected and maintained Plaintiff and the Class's PII in its computer systems. In collecting and maintaining Plaintiff's and the Class's PII, Defendant implicitly agreed that it would protect and safeguard that PII by complying with state and federal laws and regulations and applicable industry standards. Defendant was in possession of Plaintiff and the Class's PII before, during, and after the Data Breach.

20. According to the Notice of Data Breach Letter, HUB first detected suspicious activity within its network on January 17, 2023.[10] Following an internal investigation, HUB discovered the Data Breach occurred between December 2022 and January 2023.[11] HUB failed to disclose the exact dates concerning when the Data Breach began and when it ended.

21. HUB's cyber and data security systems were completely inadequate and allowed cybercriminals to obtain files containing a treasure trove of thousands of individuals highly sensitive PII, including that of Plaintiff and the Class.

22. Additionally, Defendant admitted that PII was **actually stolen** during the Data Breach confessing that the information was not just accessed, but that the "**files were**

[9] *Id.*

[10] *See* Exhibit 1.

[11] *See id.*

copied without authorization."[12] As a result of the Data Breach, Plaintiff's and the Class's personal and highly sensitive information is in the hands of cybercriminals who can place their PII for sale on the dark web or use their PII to perpetrate identity theft – if they have not already.

23. On or around August 11, 2023 – **months after the Breach first occurred** – Plaintiff and Class Members were finally notified of the Data Breach. [13]

24. Despite HUB's duties to safeguard PII, HUB did not follow industry standard practices in securing Plaintiff's and the Class's PII, as evidenced by the Data Breach.

25. In response to the Data Breach, HUB contends it has or will be taking steps to address the incident.[14] Although HUB failed to expand on what these alleged "steps" are, such steps should have been in place before the Data Breach.

26. Through the Notice of Data Breach Letter, Defendant also recognized the actual imminent harm and injury that flowed from the Data Breach and encouraged Data Breach victims to "remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports.[15]

27. Even though Social Security numbers were exposed here, cybercriminals

---

[12] *See* https://apps.web.maine.gov/online/aeviewer/ME/40/a5e4c9cb-5a57-4d11-aa3a-88c06e7a220d.shtml (Copy of Notice to Maine Residents Linked).

[13] Exhibit 1.

[14] *Id.*

[15] *Id.*

need not harvest a person's Social Security number or financial account information in order to commit identity fraud or misuse Plaintiff's and the Class's PII. Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiff's and the Class's financial accounts.

28. Plaintiff and the Class were only offered twelve months of credit monitoring services, which **does not** adequately address the lifelong harm that victims will face following the Data Breach. Indeed, the Breach involves PII that cannot be changed, such as Social Security numbers and dates of birth.

29. Even with complimentary credit monitoring services, the risk of identity theft and unauthorized use of Plaintiff's and Class Members' PII is still substantially high. The fraudulent activity resulting from the Data Breach may not come to light for years.

30. On information and belief, Defendant failed to adequately train and supervise its IT and data security agents and employees on reasonable cybersecurity protocols or implement reasonable security measures, causing them to lose control over Plaintiff and the Class's PII. Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the PII.

The Data Breach was a Foreseeable Risk of which Defendant were on Notice.

31. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in similar industries preceding the date of the breach.

32. In light of recent high profile data breaches Defendant knew or should have known that their electronic records and Plaintiff and the Class's PII would be targeted by cybercriminals.

33. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[16] The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[17]

34. Indeed, cyberattacks against the both the legal industry have become increasingly common for over ten years, with the FBI warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime."[18]

35. Therefore, the increase in such attacks, and attendant risk of future attacks,

---

[16] 2021 Data Breach Annual Report, ITRC, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.wsav.com/wp-content/uploads/sites/75/2022/01/20220124_ITRC-2021-Data-Breach-Report.pdf.

[17] *Id.*

[18] Gordon M. Snow Statement, FBI https://archives.fbi.gov/archives/news/testimony/cyber- security-threats-to-the-financial-sector.

was widely known to the public and to anyone in Defendant's industry, including HUB.

Plaintiff's Experience

36. Plaintiff received a Notice of Data Breach Letter, dated August 11, 2023, notifying her that her PII had been identified by HUB as being "accessed" and "copied" by an unauthorized actor between December 2022 and January 2023. Specifically, the letter notified her that her Social Security number was compromised in the Data Breach.[19]

37. Defendant deprived Plaintiff of the earliest opportunity to guard herself against the Data Breach's effects by failing to notify her about it for months.

38. As a result of the Data Breach, Plaintiff spent hours dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach Letter, self-monitoring her accounts and credit reports to monitor suspicious and fraudulent activity. This time has been lost forever and cannot be recaptured. Plaintiff has spent and will continue to spend considerable time and effort monitoring her accounts to protect herself from identity theft for the rest of her life.

39. Plaintiff fears for her personal financial security and uncertainty over what PII was exposed in the Data Breach. Plaintiff has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses. These feelings of anxiety are exacerbated by the fact that her children have monetary accounts tied to

[19] *See* Exhibit 1.

Plaintiff's PII as well. Thus, Plaintiff is not only concerned about her own future financial harm, but that of her children as well.

40. Plaintiff suffered actual injury in the form of damages to and diminution in the value of Plaintiff's PII—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

41. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII being placed in the hands of unauthorized third parties and possibly criminals.

42. Plaintiff has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

43. Plaintiff has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable PII; (b) the imminent and certain impending injury flowing from fraud and identity theft posed by Plaintiff's PII being placed in the hands of cyber criminals; (c) damages to and diminution in value of Plaintiff's PII; (d) loss of the benefit of the bargain with Defendant to provide adequate and reasonable data security—*i.e.*, the difference in value between what Plaintiff should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security and failing to protect Plaintiff's PII; and (e) continued risk to Plaintiff's PII, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the PII that was entrusted

to Defendant.

Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

44. Plaintiff members of the proposed Class have suffered injury from the theft of their PII that can be directly traced to Defendant.

45. As a result of Defendant's failure to prevent the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PII is used;

b. The diminution in value of their PII;

c. The compromise and continuing publication of their PII;

d. out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII; and

h. The continued risk to their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake

the appropriate measures to protect the PII in their possession.

46. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.

47. The value of Plaintiff's and the Class's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen PII openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

48. It can take victims years to spot identity theft, giving criminals plenty of time to use that information for cash.

49. One such example of criminals using PII for profit is the development of "Fullz" packages.

50. Cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

51. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and

criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and the Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

52. Defendant disclosed the PII of Plaintiff and the Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII of Plaintiff and the Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII.

53. Defendant's failure to properly notify Plaintiff and members of the Class of the Data Breach exacerbated Plaintiff's and the Class's injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

Defendant failed to adhere to FTC guidelines.

54. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of PII.

55. In 2016, the FTC updated its publication, Protecting PII: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the sensitive consumer information that they keep;

b. properly dispose of PII that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

56. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

57. The FTC recommends that companies not maintain information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

58. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

59. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to employees' PII constitutes an unfair act or practice

prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

V. CLASS ACTION ALLEGATIONS

60. Plaintiff sues on behalf of herself and the proposed nationwide class ("Class") defined as follows, pursuant to Federal Rule of Civil Procedure 23(b)(2) and (b)(3):

> **All individuals residing in the United States whose PII was compromised in the Data Breach discovered by HUB on or around January 17, 2023, and received a Notice of Data Breach Letter.**

Excluded from the Class is Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any of Defendant's officers or directors, any successors, and any Judge who adjudicates this case, including their staff and immediate family.

61. Plaintiff reserves the right to amend the class definition.

62. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

a. **Numerosity**. Plaintiff is representative of the Class, consisting of at least **479,261 individuals**, far too many to join in a single action;

b. **Ascertainability**. Members of the Class are readily identifiable from information in Defendant's possession, custody, and control;

c. **Typicality**. Plaintiff's claims are typical of class claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying

individuals about the Data Breach.

d. **Adequacy**. Plaintiff will fairly and adequately protect the proposed Class's interests. Her interests do not conflict with the Class's interests, and she has retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including lead counsel.

e. **Commonality**. Plaintiff's and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for the Class. Indeed, it will be necessary to answer the following questions:

i. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiff's and the Class's PII;

ii. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

iii. Whether Defendant was negligent in maintaining, protecting, and securing PII;

iv. Whether Defendant breached contract promises to safeguard Plaintiff's and the Class's PII;

v. Whether Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

vi. Whether Defendant's Breach Notice was reasonable;

vii. Whether the Data Breach caused Plaintiff's and the Class's injuries;

viii. What the proper damages measure is; and

ix. Whether Plaintiff and the Class are entitled to damages, treble damages, or injunctive relief.

63. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual plaintiffs are insufficient to make individual lawsuits economically feasible.

VI. CAUSES OF ACTION

COUNT I
Negligence

64. Plaintiff realleges all previous paragraphs as if fully set forth below.

65. Plaintiff and the Class's PII were entrusted to Defendant. Defendant owed to Plaintiff and the Class a duty to exercise reasonable care in handling and using the PII in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, and to promptly detect attempts at unauthorized access.

66. Defendant owed a duty of care to Plaintiff and members of the Class because it was foreseeable that Defendant's failure to adequately safeguard their PII in accordance with state-of-the-art industry standards concerning data security would result

in the compromise of that PII—just like the Data Breach that ultimately came to pass. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and the Class's PII by disclosing and providing access to this information to unauthorized third parties and by failing to properly supervise both the way the PII was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

67. Defendant owed to Plaintiff and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of their PII. Defendant also owed a duty to timely and accurately disclose to Plaintiff and members of the Class the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiff and the Class to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

68. Defendant owed these duties to Plaintiff and members of the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiff's and the Class's PII.

69. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Defendant held vast amounts of PII, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII — whether by malware or otherwise.

70. PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiff and the Class and the importance of exercising reasonable care in handling it. Especially with multiple other law firms experiencing data breaches.

71. Defendant breached its duties by failing to exercise reasonable care in protecting the PII of Plaintiff and the Class, supervising and monitoring its employees, agents, contractors, vendors, and suppliers, and in handling and securing the PII of Plaintiff and the Class which actually and proximately caused the Data Breach and Plaintiff's and the Class's injury. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and members of the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff's and members of the Class's injuries-in-fact. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and the Class have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

72. Defendant's breach of their common-law duties to exercise reasonable care and their failures and negligence actually and proximately caused Plaintiff and members of the Class actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent,

immediate, and which they continue to face.

COUNT II
Negligence *Per Se*

73. Plaintiff realleges all previous paragraphs as if fully set forth below.

74. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and the Class's PII.

75. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect customers or, in this case, employees' PII. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff's and the members of the Class's PII.

76. Defendant breached its respective duties to Plaintiff and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PII.

77. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential PII.

78. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiff's and the Class's PII and not complying with applicable industry standards as described in detail herein. Defendant's conduct was

particularly unreasonable given the nature and amount of PII Defendant collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

79. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

80. But for Defendant's wrongful and negligent breach of the duties owed to Plaintiff and members of the Class, Plaintiff and members of the Class would not have been injured.

81. The injury and harm suffered by Plaintiff and members of the Class were the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties and that its breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their PII.

82. Had Plaintiff and the Class known that Defendant did not adequately protect their PII, Plaintiff and members of the Class would not have allowed Defendant to access their PII.

83. Defendant's various violations and their failure to comply with applicable laws and regulations constitutes negligence *per se*.

84. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of PII; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen PII, entitling them to damages in an amount to be proven at trial.

85. Additionally, as a direct and proximate result of Defendant's negligence *per se*, Plaintiff and Class members have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect their PII in its continued possession.

COUNT III
Unjust Enrichment

86. Plaintiff realleges all previous paragraphs as if fully set forth below.

87. This claim is pleaded in the alternative to the breach of contract claim(s).

88. Plaintiff and members of the Class conferred a benefit upon Defendant in in the form of their PII, which allowed Defendant to render services and make revenue therefrom.

89. Defendant appreciated or had knowledge of the benefits conferred upon it by Plaintiff and the Class. Defendant also benefited from the receipt of Plaintiff's and the Class's PII, as this was used to facilitate the services it sold.

90. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of the benefit because Defendant failed to adequately protect their PII. Plaintiff and the proposed Class would not have provided their PII to Defendant and/or a client of Defendant had they known Defendant would not adequately protect their PII.

91. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and members of the Class all unlawful or inequitable proceeds received by them because of their misconduct and Data Breach.

COUNT IV
Invasion of Privacy

92. Plaintiff realleges all previous paragraphs as if fully set forth below.

93. Plaintiff and Class Members had a legitimate expectation of privacy regarding their PII and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

94. Defendant owed a duty to Plaintiff and Class Member to keep their PII confidential.

95. Defendant affirmatively and recklessly disclosed Plaintiff's and Class Members' PII to unauthorized third-parties.

96. The unauthorized disclosure and/or acquisition (*i.e.*, theft) by a third party of Plaintiff's and Class Members' PII is highly offensive to a reasonable person.

97. Defendant's reckless and negligent failure to protect Plaintiff's and Class Members' PII constitutes an intentional interference with Plaintiff's and the Class

Members' interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

98. Defendant's failure to protect Plaintiff's and Class Members' PII acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

99. Defendant knowingly did not notify Plaintiff and Class Members in a timely fashion about the Data Breach.

100. Because Defendant failed to properly safeguard Plaintiff's and Class Members' PII, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

101. As a proximate result of Defendant's acts and omissions, Plaintiff's and the Class Members' private and sensitive PII was stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages.

102. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their PII are still maintained by Defendant with its inadequate cybersecurity system and policies.

103. Plaintiff and Class Members have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard Plaintiff's and the Class's PII.

104. Plaintiff, on behalf of herself and Class Members, seeks injunctive relief to

enjoin Defendant from further intruding into the privacy and confidentiality of Plaintiff's and Class Members' PII.

105. Plaintiff, on behalf of herself and Class Members, seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

COUNT V
BREACH OF IMPLIED CONTRACT

106. Plaintiff incorporates by reference all preceding factual allegations as though fully alleged here.

107. Defendant acquired and maintained the PII of Plaintiff and the Class including their Social Security numbers and other financial information to provide services.

108. In exchange, Defendant entered into implied contracts with Plaintiff and the Class in which Defendant agreed to comply with its statutory and common law duties to protect Plaintiff's and Class Members' PII and timely notify them of a Data Breach.

109. Based on Defendant's representations, legal obligations, and acceptance of Plaintiff' and the Class Members' PII, Defendant had an implied duty to safeguard their PII through the use of reasonable industry standards.

110. Defendant breached the implied contracts by failing to safeguard Plaintiff's and Class Members' PII and failing to provide them with timely and accurate notice of the Data Breach. Indeed, it took Defendant months to warn Plaintiff and Class Member of their imminent risk of identity theft.

111. As a direct and proximate result of Defendant's breach of implied contract, Plaintiff and the Class Members have suffered damages, including foreseeable consequential damages that Defendant knew about when it requested Plaintiff's and the Class Members' PII.

112. Plaintiff and the Class have suffered injuries as described herein, and are entitled to actual and punitive damages, statutory damages, and reasonable attorneys' fees and costs, in an amount to be proven at trial.

COUNT VI
Violations of the Illinois Consumer Fraud and Deceptive Business Practices Act ("CFA"), 815 Ill. Comp. Stat. §§ 505/1, *et seq.*

113. Plaintiff realleges all previous paragraphs as if fully set forth below.

114. Plaintiff and the Class are "consumers" as defined in 815 Ill. Comp. Stat. § 505/1(e). Plaintiff, the Class, and Defendant are "persons" as defined in 815 Ill. Comp. Stat. § 505/1(c).

115. Defendant engaged in "trade" or "commerce," including the provision of services, as defined under 815 Ill. Comp. Stat. § 505/1(f). Defendant engages in the sale of "merchandise" (including services) as defined by 815 Ill. Comp. Stat. § 505/1(b) and (d).

116. Defendant engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment and omission of material facts in connection with the sale and advertisement of their services in violation of the CFA, including: (i) failing to maintain adequate data security to keep Plaintiff's and the Class Members' sensitive PII from being stolen by cybercriminals and failing to comply with applicable state and federal laws and industry standards pertaining to data security, including the FTC Act; (ii) failing

to disclose or omitting materials facts to Plaintiff and the Class regarding their lack of adequate data security and inability or unwillingness to properly secure and protect the PII of Plaintiff and the Class; (iii) failing to disclose or omitting materials facts to Plaintiff and the Class about Defendant's failure to comply with the requirements of relevant federal and state laws pertaining to the privacy and security of the PII of Plaintiff and the Class; and (iv) failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiff's and the Class's PII and other PII from further unauthorized disclosure, release, data breaches, and theft.

117. These actions also constitute deceptive and unfair acts or practices because Defendant knew the facts about their inadequate data security and failure to comply with applicable state and federal laws and industry standards would be unknown to and not easily discoverable by Plaintiff and the Class and defeat their reasonable expectations about the security of their PII.

118. Defendant intended that Plaintiff and the Class rely on its deceptive and unfair acts and practices and the concealment and omission of material facts in connection with Defendant's offering of goods and services.

119. Defendant's wrongful practices were and are injurious to the public because those practices were part of Defendant's generalized course of conduct that applied to the Class. Plaintiff and the Class have been adversely affected by Defendant's conduct and the public was and is at risk as a result thereof.

120. Defendant also violated 815 ILCS 505/2 by failing to immediately notify Plaintiff and the Class of the nature and extent of the Data Breach pursuant to the Illinois

PII Protection Act, 815 ILCS 530/1, *et seq*.

121. As a result of Defendant's wrongful conduct, Plaintiff and the Class were injured in that they never would have provided their PII to Defendant, or purchased Defendant's services, had they known or been told that Defendant failed to maintain sufficient security to keep their PII from being hacked and taken and misused by others.

122. As a direct and proximate result of Defendant's violations of the CFA, Plaintiff and the Class have suffered harm: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect PII in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

123. Pursuant to 815 Ill. Comp. Stat. § 505/10a(a), Plaintiff and the Class seek actual and compensatory damages, injunctive relief, and court costs and attorneys' fees as a result of Defendant's violations of the CFA.

VII. PRAYER FOR RELIEF

Plaintiff and the Class demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representatives, and appointing their counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen PII;

E. Awarding Plaintiff and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting such other or further relief as may be appropriate under the circumstances.

VIII. JURY DEMAND

Plaintiff hereby demands that this matter be tried before a jury.

Dated: August 25, 2023

Respectfully submitted,

/s/: William B. Federman

William B. Federman
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, OK 73120
P: 405-235-1560
F: 405-239-2112
E: wbf@federmanlaw.com